



DataRoute voice



Installation and User Manual

Version 3 – January 2011

Document Control

Date	Doc Version	Change
Dec 2010	1	1 st release of document
Dec 2010	2	Added VoIP options
Jan 2011	3	Security Options

Notices

Emergency Calls

This terminal operates using mobile signals, which cannot guarantee connection in all conditions. Therefore, you should never rely solely on the terminal equipment for essential communications such as medical or emergency services.

No responsibility is assumed by TFM for the use or reliability of the DataRoute voice when used in a situation or with other equipment not supplied or specified by TFM.

TelecomFM shall accept no liability for any error or damages of any kind resulting from the use of this document or the equipment it relates to.

The wording in this document may change from time to time. Please refer to the TelecomFM web site www.telecomfm.co.uk for the latest release.



1. Overview

The DataRoute voice is a high-speed gateway with multi-functions including:

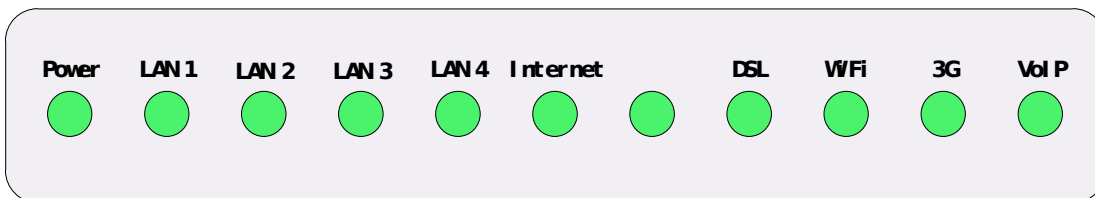
- Build-in WCDMA wireless module with speed up to 7.2Mbps;
- ADSL2/2+ modem for broadband connection;
- Four 10/100M auto-sensing Ethernet ports for wired connections;
- Build-in 802.11n enhanced WLAN complies with IEEE 802.11n draft v2.0 and backward to 802.11b/g specifications. It supports 2x2 MIMO and up to 300Mbps of bandwidth. The throughput of WLAN to LAN is more than 100Mbps;
- Integrated FXS port for voice calls;
- Supports TR-069 remote management;

2. Specification

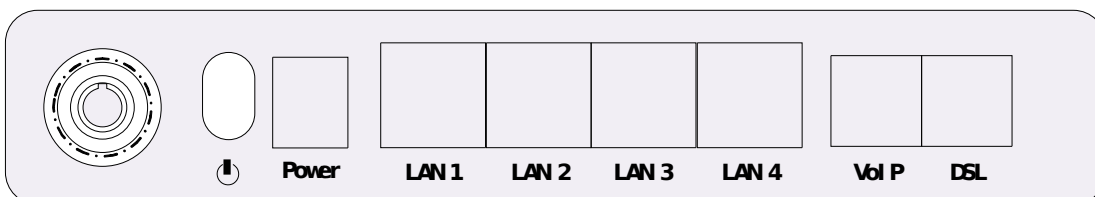
2.1 Interface Introduction

2.1.1 Indicators & Interface

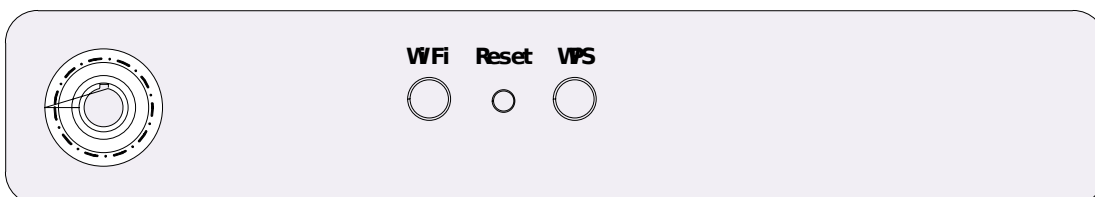
Indicators:



Interface 1:



Interface 2:

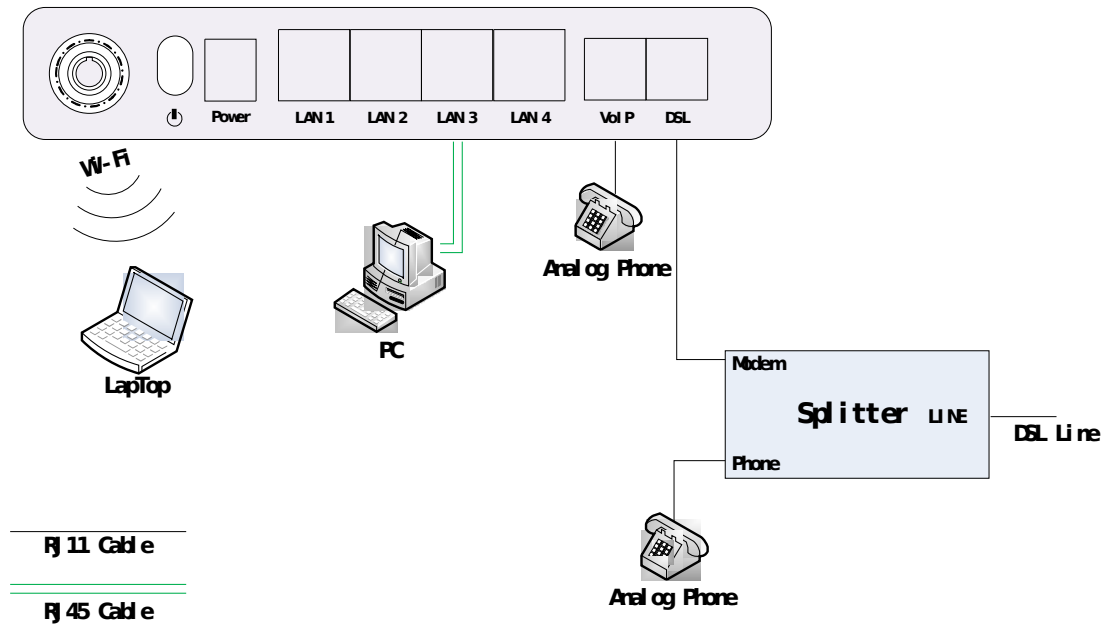


Item	Label	Description
Indicators	Power	On: Modem power up
		Off: Modem Power off
	LAN1-4	On: Ethernet is connected
		Blinking green: Ethernet Traffic flows
		Off: Ethernet is disconnected
	Internet	Blinking green: PPP/DHCP negotiation
		Solid green: PPP/DHCP up
		Quick blinking green: Tx/Rx traffic on line
	DSL	On: Modem synchronized to the DSLAM
		Quick blinking green: Modem training, but not synchronized
		Slow blinking green: Modem Idle
	Wi-Fi	On: Wi-Fi connection is available
		Blinking green: Negotiation or traffic on line
		Off: Wi-Fi connection is not available
	3G	Blinking green: Negotiation or traffic on line
		Solid green: Up
		Quick blinking green: Tx/Rx traffic on line
		Solid red: Authentication failed
Interface 1	VoIP	Off: Traffic through DSL interface
		On: The analog phone connected to VoIP off-hook
	Power	Off: The analog phone connected to VoIP on-hook
		For 12V DC power adapter
	LAN1-4	Power switch
	VoIP	LAN interface for connecting to computers
Interface 2	DSL	Connecting to analog telephones
	WiFi	Connecting to ADSL enabled telephone line
	WPS	WiFi switch
	Reset	WPS switch
		Restore to factory default settings

2.1.2 Package Contents

Item	Quantity
Power Adapter	1
Phone Line	2
RJ-45 Cable	1
Modem	1
User Manual	1
Splitter	1

2.1.3 Connection Topological Diagram



2.2 Hardware Connection

1. Use a telephone cord to connect the LINE port of the splitter with the phone socket on the wall (only if using ADSL).
2. Use another telephone cord to connect the ADSL port of the splitter with the DSL port of the DataRoute voice (only if using ADSL).
3. Connect Ethernet port of the DataRoute voice with 10/100BASE-T port of the computer using the network cable that comes with the unit.
4. Plug in the power cord, and turn on the power.

3. Configuration Guide

3.1 Default Configuration

The DataRoute voice is pre-configured with the common VCI/VPI settings. The default dial-up mode is bridge encapsulation. For bridge mode, there is no need to configure any more parameters. However, the third party dial-up software is needed for connection with the Internet.

3.2 Computer Configuration

The default IP address for DataRoute voice is: 192.168.1.1; The Subnet Mask is : 255.255.255.0. Users can configure the DataRoute voice through a web browser. The DataRoute voice can be used as a gateway and DNS server; users need to set the computer's TCP/IP protocol as follow:

1. Set the computer IP address to the same subnet as the DataRoute voice i.e. set the IP address of the PC to one in the range of 192.168.1.2 - 192.168.1.254" excluding 192.168.1.1.
2. Set the computer's gateway address to the IP address of the DataRoute voice.
3. Set the computer's Primary DNS server to the IP address of the DataRoute voice or to that of an effective DNS server.

3.2.1 Log In

Power on to start the device, then make sure your computer can PING the DataRoute voice (the factory default IP is 192.168.1.1), then run the web browser. Enter **http://192.168.1.1** in the address bar, press ENTER, and the authentication interface will pop up as below:



The default user name and password is **admin** for web log-on. Press **ENTER** or click on '**OK**' to enter the configuration interface.

Warning: Please be sure the IP of the computer network card is in the same IP range as the DataRoute voice LAN port before trying to log on (ex: 192.168.1.2 and 192.168.1.1 are in the same IP range). If the login is not displayed please check in Internet Explorer--Tools---Internet Options---Connection---LAN Setup---Proxy server, disable the function 'Proxy for LAN' and then retry.

If log on successfull, the main page will be displayed as follows:

Status	Quick	Network	Application	WLAN																								
Basic Info	<p>Basic Info</p> <table border="1"> <tr> <td>Device Model</td> <td>DataRoute voice</td> </tr> <tr> <td>Hardware Version</td> <td>V1.5</td> </tr> <tr> <td>Software Version</td> <td>1.1.2</td> </tr> <tr> <td>System Run Time</td> <td>48 seconds</td> </tr> <tr> <td>Current Time</td> <td>Thu Jan 1 00:00:47 1970</td> </tr> <tr> <td>MAC Address</td> <td>00:1a:a9:b3:04:65</td> </tr> <tr> <td>LAN Subnet IP</td> <td>192.168.1.1</td> </tr> <tr> <td>LAN Subnet Mask</td> <td>255.255.255.0</td> </tr> <tr> <td>Default Gateway</td> <td></td> </tr> <tr> <td>Primary DNS Server</td> <td></td> </tr> <tr> <td>Secondary DNS Server</td> <td></td> </tr> <tr> <td>Synchronized Time</td> <td></td> </tr> </table>				Device Model	DataRoute voice	Hardware Version	V1.5	Software Version	1.1.2	System Run Time	48 seconds	Current Time	Thu Jan 1 00:00:47 1970	MAC Address	00:1a:a9:b3:04:65	LAN Subnet IP	192.168.1.1	LAN Subnet Mask	255.255.255.0	Default Gateway		Primary DNS Server		Secondary DNS Server		Synchronized Time	
Device Model	DataRoute voice																											
Hardware Version	V1.5																											
Software Version	1.1.2																											
System Run Time	48 seconds																											
Current Time	Thu Jan 1 00:00:47 1970																											
MAC Address	00:1a:a9:b3:04:65																											
LAN Subnet IP	192.168.1.1																											
LAN Subnet Mask	255.255.255.0																											
Default Gateway																												
Primary DNS Server																												
Secondary DNS Server																												
Synchronized Time																												
Network Status																												
WAN Info																												
WLAN Status																												
Connected Devices																												
Routing Table																												
Statistics																												
VoIP Status																												

3.2.2 WAN Configuration

Please go to **Network** interface to select the **WAN Service**. Users can either edit a 3G network or an ADSL network.

Note: please power off the Gateway before inserting the SIM card.

WAN Service

Choose Add, Edit or Remove to configure a WAN service over a selected interface.
If Ports Binding is enable, only the binding port can access to the internet.
If Ports Binding is disable, all of the ports can access to the internet.

☐ Enable Ports Binding

3G Network (WAN) Service Setup

Interface	Description	Connect Mode	binding ports	APN	Dial Number	Igmp	NAT	Firewall	Status	Edit	Action
ppptd3g0	ppptd3g	AlwaysOn	none	3gnet	(null)	Disabled	Enabled	Enabled	Unconfigured		<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>

ADSL Network (WAN) Service Setup

Interface	Vpi	Vci	Category	QoS	Description	Type	binding ports	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove	edit	Action
-----------	-----	-----	----------	-----	-------------	------	---------------	-----------	-----------	--------	------	-----	----------	--------	------	--------

3.2.2.1. 3G Network Service Setup

Please go to path: Network -> WAN Device page. Check the **Enable Automatic 3G backup**, and configure the **time out all DSL link down to run 3G** – the value here is used to determine the time interval for using 3G after DSL link is down. Then click **Apply/Save**.

WAN Device Settings

please click Apply/Save to save you configure

☒ Enable Automatic 3G backup

time out all dsl linkdown to run 3G(seconds) seconds

WAN Device Select:

3G USB Dongle Select:

Then go to path: Network -> WAN Service to check the status. Please refer to the following figure.

WAN Service

Choose Add, Edit or Remove to configure a WAN service over a selected interface.
If Ports Binding is enable, only the binding port can access to the internet.
If Ports Binding is disable, all of the ports can access to the internet.

☐ Enable Ports Binding

3G Network (WAN) Service Setup

Interface	Description	Connect Mode	binding ports	APN	Dial Number	Igmp	NAT	Firewall	Status	Edit	Action
ppptd3g0	ppptd3g	AlwaysOn	none	3gnet	(null)	Disabled	Enabled	Enabled	Connected		<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>

3.2.2.2. ADSL PPPoE Configuration

Please go to path: Network -> WAN Service page. Then do the following to setup an ADSL connection.

1) Click **Add** button to configure an ATM PVC identifier;

ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI).

Notice: If the link type is EoA, it can use the PVC repeatedly though it is existent. But the PPPoA or IPoA can't.

VPI: [0-255]

VCI: [32-65535]

2) Click **Next** to select a service category; (here please choose EoA for PPPoE connection)

ATM PVC Configuration

Select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

- ☒ EoA
☐ PPPoA
☐ IPoA

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

☐ Enable VLAN

Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

☐ Enable Quality Of Service

3) Click Next to select WAN service type; (here please choose PPP over Ethernet)

WAN Service Configuration

Select WAN service type:

- ☒ PPP over Ethernet (PPPoE)
☐ IP over Ethernet
☐ Bridging

Enter Service Description: pppoe_0_0_35

Port Bind: ☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4
☐ SSID1 ☐ SSID2 ☐ SSID3 ☐ SSID4

- 4) Click **Next** to input the username and password authorized by your ISP; (here please make **Enable Fullcone NAT** checked)

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

☒ Enable Fullcone NAT

☒ Enable Firewall

☐ Dial on demand (with idle timeout timer)

☐ Use Static IPv4 Address

☐ Enable PPP Debug Mode

☐ Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

- ☐ Enable IGMP Multicast Proxy

- 5) Click **Next** to select a gateway interface;

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces

Available Routed WAN Interfaces

Current Interface

- 6) Click **Next** to select a DNS server Interface;

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

☒ Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

Available WAN Interfaces

Current Interface

7) Click **Next** to check the Summary of this connection;

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

8) Click **Apply/Save** to enable the connection.

3.2.3 Wireless Configuration

Click **WLAN** to configure the wireless feature of the modem.

- 1) Go to path: WLAN -> WLAN Basic page to enable/disable WLAN feature. Then click **Apply/Save** button;

WLAN Basic Settings

☒ Enable WLAN

☐ Disable SSID broadcast

SSID:

BSSID: 00:1A:A9:B3:04:66

Country:

Max client number:

Channel^①:

Current channel: 1

Auto Channel Timer(min)^①:

- 2) Go to path: WLAN -> WLAN Security page to set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click **Apply/Save** when done.

The default Wireless Key is **data1234** – it is strongly recommended that this be changed.

☒ Enable WLAN security

Network Authentication:

WPA Pre-Shared Key: [Click here to display](#)

WPA Group Rekey Interval:

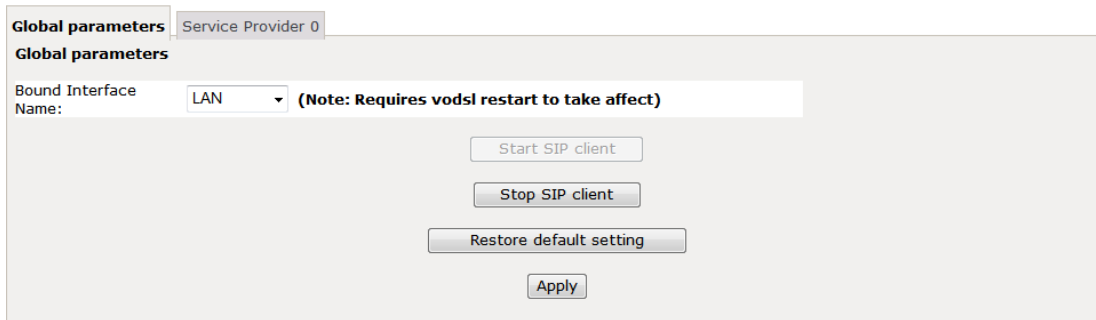
WPA Encryption^①:

WEP Encryption:

3.2.4 VoIP Configuration

3.2.4.1. Basic Settings

Go to path: VoIP -> Basic Settings page, then enter SIP parameters and click Apply to save the parameters. Click **Start SIP Client** to enable VoIP feature.



Global parameters Service Provider 0

Global parameters

Bound Interface Name: LAN (Note: Requires vodsl restart to take affect)

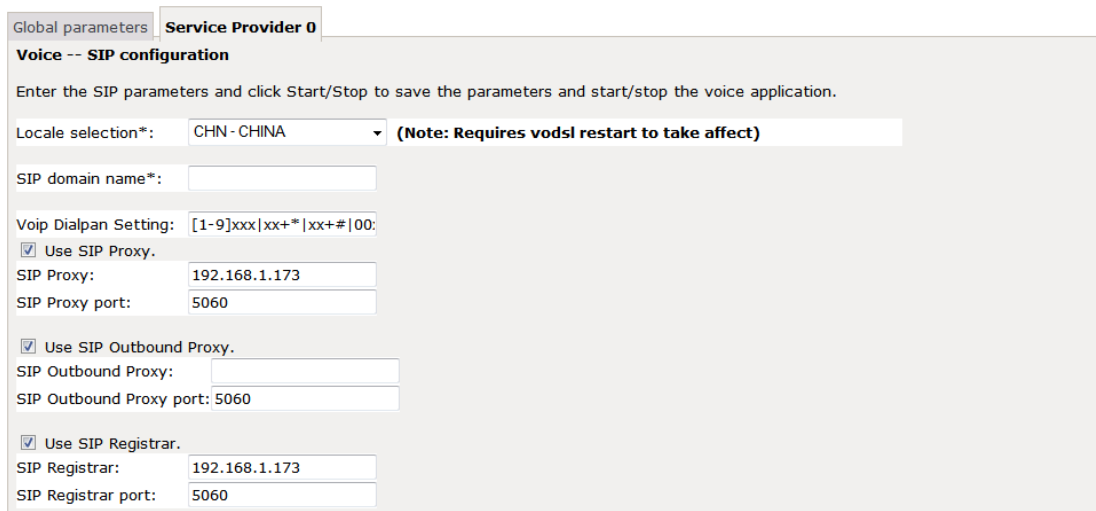
Start SIP client

Stop SIP client

Restore default setting

Apply

Bound Interface Name: Select the interface to use for the voice service, for example: ppp_0_8_35_2.



Global parameters Service Provider 0

Voice -- SIP configuration

Enter the SIP parameters and click Start/Stop to save the parameters and start/stop the voice application.

Locale selection*: CHN - CHINA (Note: Requires vodsl restart to take affect)

SIP domain name*:

Voip Dialpan Setting: [1-9]xxx|xx+*|xx+#|00:

☒ Use SIP Proxy.

SIP Proxy: 192.168.1.173

SIP Proxy port: 5060

☒ Use SIP Outbound Proxy.

SIP Outbound Proxy:

SIP Outbound Proxy port: 5060

☒ Use SIP Registrar.

SIP Registrar: 192.168.1.173

SIP Registrar port: 5060

Locale selection: choose the Location where the ADSL is used.

Preferred codec list: refers to the priority of the codec in the order left-to-right

Use SIP Proxy: enable to allow using SIP Proxy. Should be enabled while doing registration

Use SIP Outbound Proxy: enable to allow using SIP Outbound Proxy.

Use SIP Registrar: enable to register to a SIP server. Should be enabled while doing registration

SIP Account	0	1
Account Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Physical Endpt Id	0	1
Extension	1002	1003
Display name	1002	1003
Authentication name	1002	1003
Password	1002	1003
Preferred ptime	20 ▾	20 ▾
Preferred codec 1	G.711ALaw ▾	G.711ALaw ▾
Preferred codec 2	G.729a ▾	G.729a ▾
Preferred codec 3	G.723.1 ▾	G.723.1 ▾
Preferred codec 4	G.726_24 ▾	G.726_24 ▾
Preferred codec 5	G.726_32 ▾	G.726_32 ▾
Preferred codec 6	GSM_AMR_12K ▾	GSM_AMR_12K ▾

Extension: the number which will be registered to the SIP Server.

Display Name: the name which will be displayed when making outgoing calls.

Authentication Name: the authentication name which is provided by the SIP server.

Password: the password for the Extension number.

Once the configuration is done, click **Stop SIP client**, and then click **Start SIP client** to save and enable the configuration.

3.2.4.2. Advanced Settings

Go to path: VoIP -> Advanced Settings page, then configure the advanced VoIP feature.

Voice -- SIP Advanced configuration

Line	1	2
Call waiting	<input type="checkbox"/>	<input type="checkbox"/>
Call forwarding number	<input type="text"/>	<input type="text"/>
Forward unconditionally	<input type="checkbox"/>	<input type="checkbox"/>
Forward on "busy"	<input type="checkbox"/>	<input type="checkbox"/>
Forward on "no answer"	<input type="checkbox"/>	<input type="checkbox"/>
MWI	<input type="checkbox"/>	<input type="checkbox"/>
Call barring	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Call barring pin	9999	9999
Call barring digit map	<input type="text"/>	<input type="text"/>
Anonymous call blocking	<input type="checkbox"/>	<input type="checkbox"/>
Anonymous calling	<input type="checkbox"/>	<input type="checkbox"/>
DND	<input type="checkbox"/>	<input type="checkbox"/>

Call forwarding Number: set a number to use call-forwarding. Select the conditions to use call forwarding by ticking the required boxes.

Dialplan Setting: the outgoing rules which could be used to define the outgoing calls.

X refers to any digit;

| is a separator between different outgoing rules.

For example:

9XXX|(1~8)XXXXXX

This rule refers to:

Any number dialed starting with a 9 and followed by any 3 digits will go to the SIP server.

Any number dialed with 2~8 followed by any 6 digits will go to the SIP server.

Other dialed numbers will fail.

Incoming PSTN Call Routing: users could define the destination of the incoming calls.

Once the configuration is done, click **Stop SIP client**, and then click **Start SIP client** to save and enable the configuration.

4. Other Configuration

4.1 LAN Configuration

Configure the DataRoute voice's IP address and password.

4.1.1 Configuration of the DataRoute voice's IP address

As a network device, ADSL Modem has its own IP address and MAC address. The factory sets the default IP address of 192.168.1.1 and subnet mask of 255.255.255.0. The user can configure these addresses through the **Service Settings** on **DHCP** like this:

For example, change IP address to "192.168.1.10". Click **LAN**, input **IP address**: 192.168.1.10, then "subnet mask": 255.255.255.0, Press "Save" when configuration is finished.

Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Default ▾

IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

4.1.2 DHCP Configuration

1. Click **DHCP**;
2. Click **Service Settings**;
3. Define the "Start IP address" and the "End IP address" of DHCP server (for example, from 192.168.1.11 to 192.168.1.254);
4. Input the value of lease (Measured by the second, 0 indicates permanently valid);
5. Enable DHCP server, computer will set the IP Address of the PC with one of the addresses 192.168.1.2 ~192.168.1.254 (Excluding 192.168.1.1);

Note: When you use the DHCP Server, please make sure you don't have multiple DHCP Servers in one LAN.

4.2 Password Configuration

When you configure the DataRoute voice through an Internet browser, the system requires user name and password to validate access permission. The factory sets the default username of "admin" and the password of "admin". Choose Tools -> Account Settings, you can choose the username and change the password.

Access Account

Access to your DSL router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

Username:	<input type="text"/>
new name:	<input type="text"/>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>

Attention: please remember the password after change, otherwise you will need to reset the device and will lose all configuration settings.

4.3 Software Upgrade

Please go to path: Tools -> Update Software page. Click **Browse** to choose the right software. Then click **Update Software** to update.

Attention: please make sure the power of the device is stable on during the software updating process. Also, the RJ45 cable should be connected tightly between the PC and device during the software uploading process. Once updated, please press the reset button or go to path: Tools -> Factory Settings to restore the device to the new factory default settings if necessary.

Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

Software File Name:

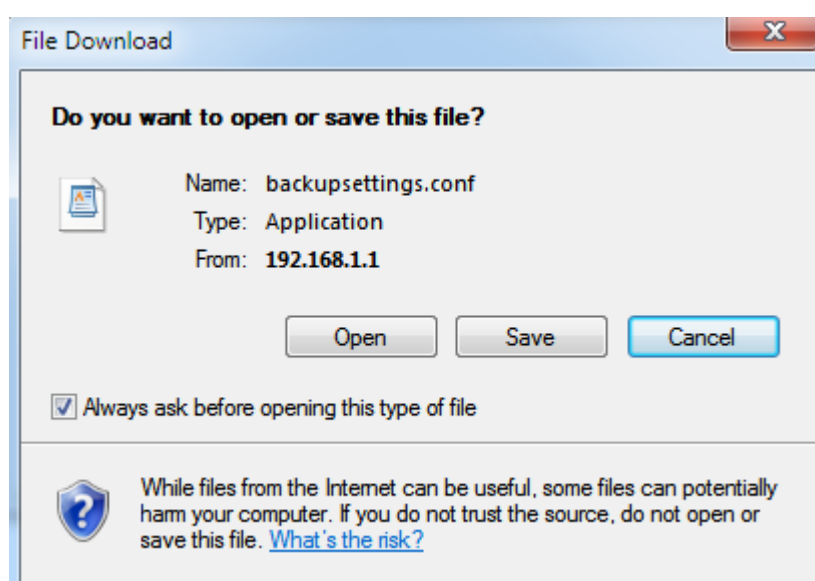
4.4 Backup Configuration

Please go to path: Tools -> Backup Settings page. Click Backup Settings button, then a File download interface pop-up. Click **Save** button to download/save current configuration of the device to the local/remote PC.

Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

Backup Settings



4.5 Restore Configuration

Please go to path: Tools -> Update Settings page. Click **Browse** button to choose a configuration file, then click **Update Settings** to restore configuration.

Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name:

4.6 Firewall

4.6.1 Firewall Settings

Please go to path: Firewall -> Firewall Settings page, check **Enable** to activate **Global firewall settings**, then click **Apply/SAVE**.

Note: three Firewall levels are supported in the device, they are:

- Low: enable basic firewall features - prevent port scanning; allow PING from WAN side; allow ICMP redirect messages from WAN side.
- Middle: in addition to Low level, prevent ICMP redirect messages.
- High: in addition to Middle level, prevent SYN Flood attack; against PING from WAN side.

Firewall Settings

Global firewall settings: ☐ Enable

Firewall level Low ▼

Apply/Save

Low

Middle

High

4.6.2 IP Filters

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Please go to path: Firewall -> IP Filters -> Incoming IP Filtering Setup.

Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
-------------	------------	------------	----------	---------------------	---------	---------------------	---------	--------

Add Remove

Click **Add** button to configure incoming IP filters. The following interface allows user to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click **Apply/Save** to save and activate the filter.

Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
Select one or more WAN/LAN interfaces displayed below to apply this rule.

- ☒ Select All
- ☒ pppd3g/ppp3g0
- ☒ br0/br0

Apply/Save

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Please go to path: Firewall -> IP Filters -> Outgoing IP Filtering Setup.

Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
-------------	------------	----------	---------------------	---------	---------------------	---------	--------

Add

Remove

Click Add button to configure outgoing IP filters. The following interface allows the user to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click **Apply/Save** to save and activate the filter.

Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

Apply/Save

4.6.3 Domain Filters

Please go to path: Firewall -> Domain Filters page. Please select the list type first then configure the list entries.

List type:

- Exclude: default accepts all the DNS except the list;
- Include: default drop all the DNS except the list;

domain Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

Exclude: default accept all the DNS expect the list

Include: default drop all the DNS expect the list

domain List Type: ☐ Exclude ☐ Include

Address	Port	Remove
---------	------	--------

Click **Add** to do the configuration after choose a domain list type. Then set the domain address and port number in the next interface. Click **Apply/Save** to add the entry to the domain filter.

Parental Control -- domain Add

Enter the domain address and port number then click "Apply/Save" to add the entry to the domain filter.

domain Address:

4.6.4 MAC Filters

Please go to path: Firewall -> MAC Filters page to setup MAC filtering. All MAC layer frames will be forwarded except those matching with any of the specified rules in the settings.

MAC Filtering Setup

All MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. Choose Add or Remove to configure MAC filtering rules.

Protocol	MAC address	Remove
----------	-------------	--------

Please click **Add** to create a filter to identify the MAC layer frames by specifying at least one condition. If multiple conditions are specified, all of them will take effect. Click **Apply** to save and activate the filter.

Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:

Source MAC Address:

(eg: 00:90:96:01:2A:3B)

4.7 QoS

Please go to path: Network -> QoS Configuration page to enable Queue Management Configuration. If **Enable QoS** checkbox is selected, a default DSCP mark should be chosen to automatically mark incoming traffic without reference to a particular classifier. Click **Apply/Save** button to save.

Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interface; The default DSCP mark is used to mark all egress packets that do not match any classification rules.

QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

☒ Enable QoS

QoS QUEUE

QoS Class

Select Default DSCP Mark

No Change(-1) ▼

Apply/Save

Please click **QoS QUEUE** button to enter the QoS Queue setup page, then click **Add** button. This screen allows you to configure a QoS queue and assign it to a specific layer 2 interface. The scheduler algorithm is defined by the layer 2 interface. Click **Apply/Save** to save and activate the queue.

QoS Queue Configuration

This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.

Note: For SP scheduling, queues assigned to the same layer2 interface shall have unique precedence. Lower precedence value implies higher priority for this queue relative to others

Click 'Apply/Save' to save and activate the queue.

Name:

Enable:

Disable ▼

Interface:

Apply/Save

Please click **QoS Class** button to enter QoS Classification Setup page, then click **Add** button to configure network traffic classes. This screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click **Apply/Save** to save and activate the rule.

Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:	<input type="text"/>
Rule Order:	Last ▾
Rule Status:	Disable ▾

Specify Classification Criteria

A blank criterion indicates it is not used for classification.

Class Interface:	LAN ▾
Ether Type:	<input type="text"/>
Source MAC Address:	<input type="text"/>
Source MAC Mask:	<input type="text"/>
Destination MAC Address:	<input type="text"/>
Destination MAC Mask:	<input type="text"/>

4.8 TR-069 Client

Please go to path: Tools -> TR-069 Client page to setup an auto-configuration server to perform auto-configuration, provision, collection and diagnostics to this device. Select the desired values and click **Apply/Save** to configure the TR-069 client options.

Note: all the parameters in the screenshot should be matched with the TR-069 Server.

TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Safe Link:	<input type="button" value="Cert Import"/>
Inform Interval:	<input type="text" value="300"/>
ACS URL:	<input type="text" value="http://200.48.229.23:70"/>
ACS User Name:	<input type="text" value="001aa92e202d"/>
ACS Password:	<input type="password" value="*****"/>
WAN Interface used by TR-069 client:	Any_WAN ▾
Display SOAP messages on serial console	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<input checked="" type="checkbox"/> Connection Request Authentication	
Connection Request User Name:	<input type="text" value="admin"/>
Connection Request Password:	<input type="password" value="*****"/>
Connection Request URL:	(null)

5. Troubleshooting

5.1 Unable to Access Internet

5.1.1 Check the Line and the Device

1. Check the power supply indicator is on - if not, make sure the connection of power supply is correct; Make sure the output of power supply is correct; Make sure the switch of the power supply is turned on ;
2. Check the LAN indicator for the PC is on - if not, check the cable connection between the PC and the DataRoute voice; Make sure that the correct cable is used;
3. Check the DSL LED to see if it is flashing. If no fast flashing is observed within 3 minutes, please check whether phone line has been correctly placed; whether ADSL filter is correctly used. If multiple extensions have been installed, make sure that the filter is installed prior to the junction box of the phone line. If the above items are confirmed and still no fast flashing of DSL LED is observed, call the ISP to query whether ADSL service has been provided on your line;
4. Check the DSL LED to see whether it is unable to change status from fast flashing to always on, or whether it changes status to fast flashing after some time of being always on. If these phenomena occur constantly, please contact your ISP with a request to check lines and signal quality;

If there is no problem in the above items, the line and the device shall be working. Problems may come from your computer configuration or device configuration.

5.1.2 Check Your Configuration

We explain here the configuration of PPPOE using Windows XP operation system as an example. For other operation systems the process is similar.

1. Enter the device manager to check if Ethernet adapter is correctly installed. If any problem exists, please re-install it;
2. Check the configuration of Ethernet adapter in PC. Try to manually set IP address that is in band 192.168.1.X without conflict.
3. Try to run command "ping 192.168.1.1" in a command prompt (Start, Programs, Accessories, Command Prompt). If the response returns "time out", please check Ethernet connection and IP settings;
4. If the DataRoute voice is reachable, try to ping a known internet IP, e.g. a DNS server: "ping 208.67.222.222".
 - If ping is reachable, there are no problems in the DataRoute voice. Please go to step 5;
 - If ping is not reachable, see step 6 and check if the configuration is correct.

5. Please try to ping a internet URL, e.g. "ping www.google.com".

- If ping is reachable, there are problems in the network settings. Please check the settings of the PC terminal, e.g. whether the security level is too high, or whether anti-virus or firewall is installed;
- If ping is not reachable, check the DNS setting of Ethernet adapter.

Note 1 : The precondition is that LAN settings in the DataRoute voice have not been modified.

Note 2 : To start a Command Prompt in Windows click on the Start menu, Programs, Accessories, Command Prompt

Note 3 : The returned values of ping command in the following format show the standard of "reachable"

```
C:\Users\Pretender>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

6. If ping of the modem is reachable but ping of the internet fixed IP is unreachable, attention should be concentrated upon device settings. Please enter the web interface following the instructions in this manual.

(1) Check first the number of connections. If more than one connection exists, for troubleshooting, delete unused connections and leave the one connection you are using.

(2) Check the connection to see whether correct "type" is selected. It's normal to choose login type of PPPoE. When you use PPPoE to login, the following information should be provided: VPI and VCI, which can be queried from your ISP, user name and password.

(3) Then make sure that "using NAT" and "default gateway" have been selected with a tick. Check whether "connect on demand" has been selected with a tick. If it is selected, the connection is activated only when traffic to the internet arrives. If not selected, check "keep connection", which should be set to 0 if you demand to keep connection

Make sure that the above parameters are saved after configuration.